

Conseil d'État

N° 433311

ECLI:FR:CECHR:2020:433311.20201104

Mentionné aux tables du recueil Lebon

10ème - 9ème chambres réunies

Mme Isabelle Lemesle, rapporteur
M. Alexandre Lallet, rapporteur public
SCP BARADUC, DUHAMEL, RAMEIX, avocats

Lecture du mercredi 4 novembre 2020

REPUBLIQUE FRANCAISE
AU NOM DU PEUPLE FRANCAIS

Vu la procédure suivante :

Par une requête sommaire, un mémoire complémentaire et deux mémoires en réplique, enregistrés les 5 août 2019, 5 novembre 2019, 5 août 2020 et 3 septembre 2020 au secrétariat du contentieux du Conseil d'Etat, la société d'étude et de réalisation de gestion immobilière de construction (SERGIC) demande au Conseil d'Etat :

1°) d'annuler la délibération n° SAN-2019-005 du 28 mai 2019 par laquelle la formation restreinte de la Commission nationale de l'informatique et des libertés (CNIL) a prononcé à son encontre une sanction pécuniaire d'un montant de 400 000 euros et ordonné la publication de sa délibération pendant une durée de deux ans, avant anonymisation ;

2°) d'enjoindre à la CNIL de publier la décision à venir du Conseil d'Etat dans les mêmes formes que la délibération attaquée ;

3°) de mettre à la charge de la CNIL la somme de 5 000 euros au titre de l'article L. 761-1 du code de justice administrative.

Vu les autres pièces du dossier ;

Vu :

- le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ;
- la loi n°78-17 du 6 janvier 1978 ;
- le code de justice administrative ;

Après avoir entendu en séance publique :

- le rapport de Mme Isabelle Lemesle, conseiller d'Etat,
- les conclusions de M. Alexandre Lallet, rapporteur public ;

La parole ayant été donnée, avant et après les conclusions, à la SCP Baraduc, Duhamel, Rameix, avocat de la Société Sergic ;

Considérant ce qui suit :

1. Il résulte de l'instruction que la Commission nationale de l'informatique et des libertés (CNIL), à la suite d'un signalement faisant état de l'existence d'un défaut de sécurité permettant à des tiers non autorisés d'accéder aux données personnelles de candidats à la location d'un bien immobilier ayant téléchargé des documents sur le site www.sergic.com, a diligenté le 7 septembre 2018 une mission de contrôle en ligne sur le traitement mis en oeuvre par la société d'étude et de réalisation de gestion immobilière de construction (SERGIC), à l'occasion de laquelle a été constaté un manquement aux dispositions de la loi du 6 janvier 2018 relative à l'informatique, aux fichiers et aux libertés et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, RGPD, dont la société a été informée le jour même. Lors d'une mission de contrôle effectuée sur place le 13 septembre 2018, la délégation de la CNIL a constaté qu'il n'avait pas été porté remède à ce défaut de sécurité. La présidente de la CNIL a alors engagé une procédure de sanction à l'encontre de la société SERGIC. Par une délibération n°2019-995 du 28 mai 2019, la

formation restreinte de la CNIL a infligé à la société SERGIC une amende de 400 000 euros et décidé de rendre cette sanction publique pendant une durée de deux ans à compter de sa publication avant anonymisation.

2. En premier lieu, l'article 44 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans sa rédaction applicable au litige, devenu l'article 19 de la même loi, dispose que : " I. - Les membres de la Commission nationale de l'informatique et des libertés ainsi que les agents de ses services habilités (...) / En dehors des contrôles sur place et sur convocation, ils peuvent procéder à toute constatation utile ; ils peuvent notamment, à partir d'un service de communication au public en ligne, consulter les données librement accessibles ou rendues accessibles, y compris par imprudence, par négligence ou par le fait d'un tiers, le cas échéant en accédant et en se maintenant dans des systèmes de traitement automatisé de données le temps nécessaire aux constatations ; ils peuvent retranscrire les données par tout traitement approprié dans des documents directement utilisables pour les besoins du contrôle (...) ". Il résulte de ces dispositions que pour retranscrire les données d'un service de communication au public en ligne, les membres de la CNIL et ses agents habilités, dans le cadre de leurs missions de contrôle, peuvent télécharger les fichiers rendus accessibles par un défaut de sécurité. Il s'ensuit que c'est à bon droit que la formation restreinte de la CNIL a rejeté la demande de la société SERGIC tendant à faire déclarer nulles les constatations opérées en ligne par les agents de la CNIL le 7 septembre 2018.

3. En deuxième lieu, aux termes de l'article 45 de la loi du 6 janvier 1978, dans sa rédaction applicable au litige, devenu l'article 20 de la même loi : " I. - Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi. / II. - Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible de faire l'objet d'une mise en conformité, prononcer à son égard une mise en demeure, dans le délai qu'il fixe : (...). / III. - Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, (...) le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes : / (...) 7° A l'exception des cas où le traitement est mis en oeuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83 (...) ". Il résulte clairement de ces dispositions que le prononcé d'une sanction par la formation restreinte de la CNIL n'est pas subordonné à l'intervention préalable d'une mise en demeure du responsable du traitement ou de son sous-traitant par le président de la CNIL. Il s'ensuit que le moyen tiré de ce que le président de la CNIL aurait méconnu les dispositions du III de l'article 45 de la loi du 6 janvier 1978 en saisissant la formation restreinte sans adresser à la société requérante une mise en demeure préalable, ne peut qu'être écarté.

4. En troisième lieu, aux termes de l'article 5 du RGPD : " 1. Les données à caractère personnel doivent être : (...) / e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en oeuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) (...) ". Il résulte de l'instruction, d'une part, que la finalité pour laquelle les données à caractère personnel des candidats à la location sont conservées et traitées par la société SERGIC est le suivi des demandes de location d'un bien immobilier et, d'autre part, que les missions de contrôle de la CNIL ont révélé que les documents transmis par les personnes désirant louer un bien immobilier étaient conservées, sans archivage intermédiaire, pour tenir compte du délai de prescription de six ans des actions en discrimination. Dès lors, en estimant que la durée de conservation des données excédait dans des proportions importantes celle nécessaire à la réalisation de la finalité du traitement, sans qu'aucune solution d'archivage intermédiaire, qui aurait permis de conserver les données nécessaires à la gestion d'un éventuel contentieux, n'ait été mise en place, la formation restreinte de la CNIL n'a pas méconnu les dispositions du e) du 1° de l'article 5 du RGPD, ni entaché sa délibération d'erreur manifeste d'appréciation ni d'insuffisance de motivation.

5. En dernier lieu, aux termes de l'article 83 du RGPD : " 1. Chaque autorité de contrôle veille à ce que les amendes administratives imposées en vertu du présent article pour des violations du présent règlement visées aux paragraphes 4, 5 et 6 soient, dans chaque cas, effectives, proportionnées et dissuasives. / 2. (...) Pour décider s'il y a lieu d'imposer une amende administrative et pour décider du montant de l'amende administrative, il est dûment tenu compte, dans chaque cas d'espèce, des éléments suivants : a) la nature, la gravité et la durée de la violation, compte tenu de la nature, de la portée ou de la finalité du traitement concerné, ainsi que du nombre de personnes concernées affectées et le niveau de dommage qu'elles ont subi ; b) le fait que la violation a été commise délibérément ou par négligence ; c) toute mesure prise par le responsable du traitement ou le sous-traitant pour atténuer le dommage subi par les personnes concernées ; d) le degré de responsabilité du responsable du traitement ou du sous-traitant, compte tenu des mesures techniques et organisationnelles qu'ils ont mises en oeuvre en vertu des articles 25 et 32 ; e) toute violation pertinente commise précédemment par le responsable du traitement ou le sous-traitant ; f) le degré de coopération établi avec l'autorité de contrôle en vue de remédier à la violation

et d'en atténuer les éventuels effets négatifs; g) les catégories de données à caractère personnel concernées par la violation; h) la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable du traitement ou le sous-traitant a notifié la violation; (...)/3. Si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence plusieurs dispositions du présent règlement, dans le cadre de la même opération de traitement ou d'opérations de traitement liées, le montant total de l'amende administrative ne peut pas excéder le montant fixé pour la violation la plus grave. /(...) 5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu:/ a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 (...)"

6. Il résulte de l'instruction que les manquements constatés par la formation restreinte de la CNIL consistaient d'une part, en un défaut de sécurité du site www.sergic.com permettant, comme il a été dit au point 1, à des tiers non autorisés d'accéder, au moyen d'une simple modification de liens URL, à plusieurs centaines de milliers de documents téléchargés par plusieurs dizaines de milliers de candidats à la location de logement, tels que des bulletins de salaires, des avis d'imposition, des justificatifs d'identité ou des actes de mariage ou de divorce, qui contiennent des données à caractère personnel lesquelles, sans être nécessairement des données sensibles au sens du RGPD, concernent la vie privée des personnes, et d'autre part, en une conservation de ces données pendant une durée excessive au regard de la finalité poursuivie par leur traitement. Eu égard à la nature et à la gravité des manquements constatés qu'il aurait été possible de prévenir par des mesures simples de sécurité, comme l'authentification des utilisateurs du traitement, ainsi que par des mesures d'archivage, aux moyens dont disposait la société pour y remédier et au délai avec lequel elle a apporté les mesures correctrices nécessaires, la formation restreinte de la CNIL n'a pas infligé à la société SERGIC une sanction disproportionnée en prononçant à son encontre une sanction pécuniaire d'un montant de 400 000 euros, représentant moins de 1% de son chiffre d'affaires pour l'année 2017 et 4% du plafond des sanctions, accompagnée, pour en assurer le caractère dissuasif et informer les utilisateurs du traitement concerné des risques auxquels ils ont été confrontés, d'une sanction complémentaire consistant en sa publication pendant une durée de deux ans avant son anonymisation.

7. Il résulte de tout ce qui précède que la société SERGIC n'est pas fondée à demander l'annulation de la délibération qu'elle attaque. Sa requête doit être rejetée, y compris ses conclusions tendant à l'application de l'article L. 761-1 du code de justice administrative.

D E C I D E :

Article 1er : La requête de la société d'étude et de réalisation de gestion immobilière de construction est rejetée.

Article 2 : La présente décision sera notifiée à la société d'étude et de réalisation de gestion immobilière de construction et à la Commission nationale de l'informatique et des libertés.
